

Đĩ#à i ±#á#####>###þÿ

[illegible]

###!###"#####\$###%###&###'###(###)###*###+###,###-
###.###/###0###1###2###3###4###5###6###7###8###9###:###;###<###=###>###?
###@###A###B###C###D###E###F###G###H###I###J###K###L###M###N###O###P###Q###R###b
ÿÿT###U###V###W###X###Y###Z###[###\###]###^###_###`###a###b###c###d###e###f###g
###h###i###j###k###l###m###n###o###p###q###r###s###u###ýÿÿv###w###x###y###z###{
###|
###}###~###[]####R#####
#####ÿÿÿÿÿÿ#####QH#####À#####F#####<nB°½#[###]#####P#P#4#0#####

###ÿÿÿ#####ÿÿÿ#####k i#####S#u#m#m#a#r#y#I
#n#f#o#r#m#a#t#i#o#n#####(###ÿÿÿÿÿÿÿÿÿÿÿ#####
#####S###ð[]#####C#u#r#r#e#n#t#
#U#s#e#r#####ÿÿÿ#####
#####Pí#####F#
##i k#f#E#####[]#####N[]##À###f[]##8###&[]##### ^[]#

^##&###ð##@####V#####V##`###V##&###¶##"###Û##
###p#####4## ###L#####l#####
###>#####^#####^#####^##&###l##"###
'#####ì#####ì#####ì#####ì##&###ú##"#####:#####:#####
:#####:##&###H##"###n@#~x#####<#####D#####
\\#####z#####¼#####³/₄#####ø##*###ò##H###@##d##v##¼##v##
##v##v##v##v##0##|#####-##"###³/₄#####à##

##ö#####ü##

##

!

'[]##*## 3[]##x## 1[]##[]## Õ#####ÿÿÿ#####

#|Àø#öDøë □#####3º
´ÿÿ###3º□#C#Dù#ÿD#-ÿD#####@D##ôÅ##
Ô##### #|À#4ø,#÷ú□#####3º|ÿÿ###3ºT
#|À#TôÅ#Lÿl#####3ºLÿÿ###3º\$ #¼À#@9###x#####3º#ÿÿ###3¹ô @D# #,#□
-#####ÿÿ##### @D# #,#à
-#####ÿÿ#####C#D#%#Å#|#Ä#####@D#%#Ô#|
#Ô##### #¼À#\$#Ô#×
|#####3¹Ïÿÿ###3¹¼ #¼À#\$#ô#×#□#####3¹ÿÿ###3¹t
#¼À#\$#ä#×#□#####3¹lÿÿ###3¹D#@D#%#´#|#´##### #|Áøäÿôÿ#
|#####3¹8ÿÿ###3¹4#@D#t#µ#t
□#####@D#ä#u#ä
□#####@D#Å#□#Å
□##### #|À###d#®#□#####3,üÿÿ###3,ô
##Døpù#ù#ù#####ÿÿ#####@D#□#µ#□
□##### #¼À#t#d#X#□#####3,´ÿÿ###3,□
#¼À#T#d#8#º#####3,□ÿÿ###3, \ #¼À###d###0#####3,Tÿÿ###3, ,#@D#ô#□#ô
□##### #|À#□ø# \#□#####ÿÿ###3·ü
#|À#d#d###s#####ÿÿ###3·D#@D#t#µ#t#####@D#□#µ#□#ô#####
#####@D#ä#u#ä#ô#####@D#ô#U#ô
□#####@D#Ä#U#Ä
□#####@D#t#µ#t#Ä#####@D#□#µ#□#ä#####
#####@D#ä#□#ä#ä#####@D#ô#å#ôd#####@D#Ä#u#Ä
Ä#####@D#t#u#t#¼#####@D#t ##t
4#####@D#t □#t Ä#####@D#t
%#t
T#####@D#□#¥#□#ô#####@D#□ 5#□
d#####@D#□ Ä#□ ô#####@D#□
U#□
□##### @D#Döôÿ´p#####ÿÿ##### #### # @#####(##0##0###@##
@#####(##0##0###@##

d#d#c#d#####(##0#0#d#d#C #### # #@#####(##0#0###@## #### # #@#####(##0#0###@## ####
#@#####(##0#0###@## #### # #@#####(##0#0###@## ####ø# ###@####(##0#0###@##
#*Û#` \#####(##0#0#!çP## #### # #@#####(##0#0###@## #### # #@#####(##0#0###@##
#@#####(##0#0###@#####
##[]##
###İ#[]###ø#öløÛ hÿÿ####ÿÿ#####ÿ*#ÿÿ#d#####d#####/Explaining &
Recovering from Computer Break-ins##

###/#####/#####/#####/#ÿ¥#ÿÿ#d#####U#####İ#[]####DøT#ç
úhÿÿ####ÿÿ####ÿ¥#ÿÿ#d#####d#####Impact#

#####ÿ*#ÿÿ#d#####U#####İ#[]####dôì#<
ÿDÿÿ####ÿÿ####ÿ*#ÿÿ#d#####d#####CDoD Information Security improved by
DERBI providing expertise to widely distributed, minimally trained System
Administrators Crisis response improved by current information distributed via
databaseDowntime and exposure minimized by nullifying current attacksSituation
awareness raised by reporting coverage and accuracy,#

###C#####!
#####^#####1#####
#####C#####@ÿ¥#ÿÿ#d#####U#(
#####I@ÿ¥#ÿÿ#d#####U#(#####>@ÿ¥#ÿÿ#d#####U#(#####=@ÿ¥#ÿÿ#d#####
#U#(#####P#a#ó#Pÿÿ####ÿÿ####ÿ¥#ÿÿ#d#####d#####
Scheduleù#

#ÿ×#ÿÿ#d#####U#####□#□####4#ü#Ç
Tÿÿ####ÿÿ####ÿ×#ÿÿ#d#####d#####FY00#

#####ÿ¥#ÿÿ#d#####U#####
#tÿÿ####ÿÿ####ÿ¥#ÿÿ#d#####d#####FY99#

#####ÿ¥#ÿÿ#d#####U#####
#####4#

#Ç#dÿÿ####ÿÿ####ÿ×#ÿÿ#d#####d#####FY98#

#####ÿ¥#ÿÿ#d#####U#####Ì######(#
#\ÿÿ####ÿÿ####ÿ¥#ÿÿ#d#####d#####Exploit database#

#####

#####ÿÿ#d#####g#4#####
ÿÿ#d#####d#####Explanation and reporting#

#####

#####ÿ×#ÿÿ#d#####U#####ÿ×#ÿÿ#d#####U#####
#####d#(##ÿÿ#####ÿÿ#####ÿ×#ÿÿ#d#####d#####-Evidential correlations
among indicators##

- ##### -

-
#####ÿŸ#d#####U#####ÿŸ#d#####U#####
#####ÿŸ#d#####d#####)Intrusion indicators knowledge
base##

###)#####)###

#####)#####ÿ¥#ÿÿ#d#####a#####ÿ¥#ÿÿ#d#####a#####
#####¥øÇ#?#Gÿÿ#####ÿ¥#ÿÿ#d#####d#####?Artificial Intelligence
Center, SRI International: Mabry Tyson##

###?#####?#####?#####?

#ÿ¥#ÿÿ#d#####d#####□#□####□#□#ô#9ÿÿ####ÿÿ####ÿ¥#ÿÿ#d#####d#####

##Recovery and repair##

#####

#####ÿ*#ÿÿ#d#####d#####Ì####øôÿüþ÷

Tÿÿ####ÿÿ####@ÿ*#ÿÿ#d#####V#(#####

New IdeasForensic analysis of intrusions uses database of current
vulnerabilities and exploitsAnalysis drives explanation-based recommendation of
steps for recovery and preventionAutomated reporting from sites updates database
used in analyzing subsequent attacks#

#####

###

#####U#####

#####A#####

#ÿ¥#ÿÿ#d#####V#(#####V@ÿ¥#ÿÿ#d#####V#(#####V@ÿ¥#ÿÿ#d#####V#(####
###T@ÿ¥#ÿÿ#d#####V#(#####.#.##ÿÿ##ý#####0`#2######
##Đöxújp0######ÿý##### #ÅÿvùÅ #####ÿý###
%[]@#####0#####L#[]###ÿ[]ùÿ []#á###

#####ÿ*#ÿÿ#d#####d#####

#####ÿÿ##áÿ####0#U0Hy#####3¹/₄

#4#@#####
#####%P#####

#####3¹/₄\#####ÿÿÿÿ#####

#␣ÂùØb¼û##\#####%␣``ÿÿ###%␣ô #### #
#@#@###(#0#0###@#####*#####M#␣###ùèpâû##4ÿÿ#\$##ÿÿ#####ÿ¥#ÿÿ#d#####U##
#####Title #

#####\$#####ÿ¥#ÿÿ#d#####U#####
##ÿÿàj#### /##/1#####
##Döxújp0#[]#####ÿý#####®#####ÿÿÿÿĐ¹#####H##Ho####
####3¼(#####4 #4
0#####ÿÿÿÿ#####

o#####ÿÿÿÿÀ#####©#<"#####3¹/₄d#####
#####ÿÿÿÿ#####

#####D#####%###"#####ÿÿÿÿÃ#####1šà#####\$#3¼####!
#####&#####~x#6#B###+###ÿ

```
#ÿÿÿÿ#B###6###+#####i#[]###5#A###+i#À#y%PostScript Hack by Mike Brors
12/7/90/DisableNextSetRGBColor      {      userdict begin      /setrgbcolor
      {      pop      pop      pop      userdict begin
      /setrgbcolor systemdict /setrgbcolor get def      end      } def end
} bind def/bcarray where {      pop      bcarray 2 {      /da 4 ps div def      df
setfont gsave cs wi      1 index 0 ne{exch da add exch}if grestore
setcharwidth      cs 0 0 smc da 0 smc da da smc 0 da smc c      gray
      { gl}      {1 setgray}ifelse      da 2. div dup moveto show      }bind put
} if%% Used to snap to device pixels, 1/4th of the pixel in./stp { % x y pl x
y      % Snap To Pixel, pixel (auto stroke adjust)      transform
      0.25 sub round 0.25 add exch 0.25 sub round 0.25 add exch itransform}
bind def/snapmoveto { % x y m -      % moveto, auto stroke adjust      stp
moveto} bind def/snaplineto { % x y l -      % lineto, auto stroke
adjust      stp lineto} bind def## #[]#####
#6#B###*#####"#7#q### #[]#"#8#¼### # #i#¼#####
#####"#t#½#####ø###õ###ó###ó###ü#####úô#####õ#####û#
##÷ÿ###ÿ#####û#####
```

###ÿ#####ÿ###ÿ#####»»»»»»###
#6#B###*#[]#
#8#¼#8#¼# #£# #¾#q#[]#8#£#t#È#t#¾#t#Â#s#Â#p#Â#f#Â#Z#Â#N#Â#G#Ã#D#Å#C#È#8#Ã#8#·#9#
'#:#±#;#®#:#³#9#©#9#¼#:#£#>#£#C#£#D#¼#D#©#B#®#F#·#N#º#Z#º#f#º#p#º#s#º#t#º#t#¾#"#
8#¼### #¿# #i#####i#¶#####@# # #i#¼#####
#####"#t#¾#####ø###õ###ó###ó###ü#####úô#####õ#####
####û###÷ÿ###ÿ#####û#####

[illegible]

```
#6#B###*#[]#
#9#q#9#q# #£# #¾#q#[]#;#[]#[]#[]#[]#[]#[]#[]#~#[]#o#[]#`#[]#S#[]#I#[]#F#[]#E#[]#?
#[]#=#[]#<#[]#;#[]#;#[]#;#[]#?#[]#?#[]#?
#[]#Q#[]#Q#[]#A#[]#E#[]#F#[]#J#[]#T#[]#a#[]#p#[]#~#[]#[]#[]#[]#[]#[]#[]#[]#[]#[]#"#9#q### #¿# #i##
###i#¶#####Q# # #i#¤#####
#####"#[]#[]è###à###ç###û##üû##øÿ##÷ÿ##ÿ#####
ÿ###ÿ ##ÿ##### #£# #¾###
#6#B###*#####i#¶#####Q#####i#¶#####@#####p#[]#;#[]#[]#[]#[]#[]#[]#[]#~#[]#
#o#[]#`#[]#S#[]#I#[]#F#[]#E#[]#?#[]#=#[]#<#[]#;#[]#;#[]#;#[]#?#[]#?#[]#?
#[]#Q#[]#Q#[]#A#[]#E#[]#F#[]#J#[]#T#[]#a#[]#p#[]#~#[]#[]#[]#[]#[]#[]#[]#[]#[]#[]#[]#"#¿# #i#####
#i#¶#####Q# # #i#¤#####
#####"#[]#[]#####¹#####ÿ###üû##ÿ#####óp##### #£# #¾###
#6#B###*#####i#¶#####Q#####i#¶#####@#####p#"#<#[]#[]#[]#[]#[]#F#[]#@#[]#>#[]#=#[]#
#<#[]# #¿# #i# # #i#¤#####
#####"#[]#[]####ÿ#####p###ÿ###ô###öÿ##ÿÿ##ÿÿü###p#####ü#####p###ù###
#####
#####ÿÿ###
#6#B###*#[]#
#9#q#9#q# #£# #¾#q#^#[]#r#®#[]#[]#[]#£#[]#¥#[]#§#[]#ª#[]#-
#[]#®#{#~#v#<#t#©#r#`#r#¥#r#¤#s#¤#v#i#|# #[]# #[]#[]#[]#[]#[]#[]#[]#[]#"#9#q### #¿# #i##
###i#¶#####Q# # #i#¤#####
#####"#[]#[]####ÿ#####p###ÿ###ô###öÿ##ÿÿ##ÿÿü###p#####ü#####p###ù###
#####
##### #£# #¾###
#6#B###*#####i#¶#####Q#"#[]#[]###i#¶#####@#####p#^#[]#r#®#[]#[]#[]#£#[]#¥#[]#§#[]#
#ª#[]#[]#[]#®#{#~#v#<#t#©#r#`#r#¥#r#¤#s#¤#v#i#|# #[]# #[]#[]#[]#[]#[]#[]#[]#[]#"#¿# #i# # #
i#¤#####
#####"#§#[]ø###÷p##ÿü#####
```

û###þ#####LÍLÐÿÿ###

#6#B###*#[]#

#9#q#9#q# #£# #¾#q#6#[]#t#<#[]#£#[]#ª#[]#<#[]#<#{#`#u#|#t#|#w#¥#{#£#[]#[]#[]#£#[]#"#9#q##

#¿# #i#####i#[]##### # #i#¼#####

#####"#§#[]ø###÷þ##ýü#####

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

ÿ##33ÿÿîî##33ÿÿ##33ÿÿff##33ÿÿ33##33ÿÿ####33îîÿÿ##33îîîî##33îî##33îîff##33îî3
3##33îî####33ÿÿ##33ÿÿîî##33ÿÿ##33ÿÿff##33ÿÿ33##33ÿÿ####33ffÿÿ##33ffîî##33ff
##33ffff##33ff33##33ff####3333ÿÿ##3333îî##3333ÿÿ##3333ff##333333##3333####33##ÿ
ÿ##33##îî##33##ÿÿ##33##ff##33##33##33#####ÿÿÿÿ##ÿÿîî##ÿÿÿÿ##ÿÿff##ÿÿ3
3####ÿÿ#####îîÿÿ#####îîîî#####îîÿÿ#####îîff#####îî33#####îî#####ÿÿ#####îî#####
ÿÿ#####ÿÿff#####ÿÿ33#####ÿÿ#####ffÿÿ#####ffîî#####ffÿÿ#####ffff#####ff33#####ff#####33ÿ
ÿ####33îî####33ÿÿ####33ff#####3333####33#####ÿÿ#####îî#####ÿÿ#####ff#####3
3##îî#####ÿÿ#####»»#####a a#####ÿÿ#####ww#####UU#####DD#####" "#####
#####îî#####ÿÿ#####»»#####a a#####ÿÿ#####ww#####UU#####DD#####" "#####
#####îî#####ÿÿ#####»»#####a a#####ÿÿ#####ww#####UU#####DD#####" "#####
###îîîîîî##ÿÿÿÿÿÿ##»»»»»»##a a a a a a#####ÿÿ#####www#####UUUUUU#####DDDDDD##" " " " "#####
#####ÿÿÿÿ#####C###'#\$#,#C###'##ÿÿ#C#ÿÿÿÿÿÿ#ÿÿ###C#ÿÿÿÿÿÿ#ÿÿ###C#ÿÿÿÿÿÿ#ÿÿ###C#ÿÿÿÿÿÿ#
#

[illegible]

#####

#[]#[]#ö#[]#####"#[]#[]### #[]#i#[]##ÿi[][]ÿÿR###ÿÿ#####,# #÷#Impact####÷#

###.#####í#è#í#è#+[]\$#D## #[]# #[]#+###E## #[]# #[]#(#í#[]#R## #[]# #[]#*##B# #[]# #[]
#*## ###R##)##I## #[]# #[]#####i#[]#

#####

#[]#[]#<#0#"#[]#[]### #[]#i#[]##yók[]##u###yy[][],##*Ý#Arial Black##*Ý##

##S# diagnosis,## #######i##

```
##[]#¿#ã#"##[]### []#i#[]##ÿó[]###{###ÿÿ[]####(#°#[]#xplanation,# []# []#####i
#[]#
```

#####

#Ä# #Ñ#İ#"#Ä# ## #i# ##ÿò##q##ÿÿ#####+###ecovery# # # #####i#

#0#ä#½#"#0# ## #i# ##ÿò¼###i###ÿÿ#####+###reak-# # # #####i#

#####

#æ# #÷#ª#"#æ# #### # #i# ##ÿò·##_###ÿÿ####(#ó# #ns## # # # #####i# #

#Â#Ó#Ð#ë#"#Â#Ó### #[]#i#[]##ÿö[]#ÿÿ[]###ÿÿ[]###
#[]#ÿ##PICT#2{È###(ÿÿÿÿ#3'-#3³0#####2|
##3¼0###3¼È#####)###2ÎL##[]ÿ#####3ÑP#####*###+#0ÍH#4-p#3¼##### #
#@#@#`#`#[]#[]###@###0###0# #Ð#@#ð#`###[]###@###0###0# ###@#8#`#X#[]###@###H###0#
###@#8#`#X#[]###@###[]##2Û[]##[]ÿ#####3Ñ[]#####-
#####.#####/#####0##s[]#####D#8#)à#<0i#(U0©s##f /
W"P"i#îN[]p#Aî## 0R@J#X0g\$/o#
##Ho##`qHo###
###20i#

#)à W"P"i#ìN□Ho##©rHo# // # / #
W"P#####iøÿý#####d#d#####d#d#d###*Â@#
%###□#####XÿÿÿÿÿÿY#####h□h□h#Y#####DaG□[ýò#3##®#####üì##(ö##ÎØÎØÎØÿý#####
##d#d#####d#d#d###*Ã□#
%###□#####XÿÿÿÿÿÿY#####h□h□h#Y#####DaG□[ýò#3##®#####üì##(ö##ÎØÎØÎØÿý#####
##d#d#####d#d#d###ôÉ#####XÿÿÿÿÿÿY#####□□□□□#@###XX#
#üü##((#B##==èè#?##ßßÊÊ#
%êêìì^ÿÿ#####d#d#####d#d#d###Đđ#####XÿÿÿÿÿÿY#####
□□□□□#@###XX##üü##((#B##==èè#?##ßßÊÊ#
%êêìì^ÿÿ#2□ü##ÿÿ#####3Ńp#####4#####5#####6#####7#3ÌÀ#3Ã##3¼□##M#□####\$###
, ##### , ##### , ##### , #####ÿ¥#ÿÿ#d#####U#####
##ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####
#####ÿ¥#ÿÿ#d#####d#####L#□####
#####@ÿ¥#ÿÿ#d#####d#####
####@ÿĐ#ÿÿ#d#####d#####@ÿ¥#ÿÿ#d#####d#####@ÿĐ#ÿÿ#d#####d##
#####@ÿ¥#ÿÿ#d#####d#####L#□####

#####

#####

#####

#####

#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####
#d#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####ÿÿL#[]#####
#####T¥#####d#####d##ÿp####
##T¥#####d#####d##ÿp#####T¥#####d#####d##ÿp####
#####T¥#####d#####d##ÿp#####T¥#####d#####d##ÿp####
#####T¥#####d#####d##ÿp#####Ï#[]#####
#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####ÿ¥#
ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####ÿ¥#ÿÿ#d#####d#####
##0#0####[]#####Times New
Roman###;####ÿÿ#@#Geneva###=####ÿÿ#>#Arial###?#####@#Times###A#####[]##2Ú
'##[]ÿ#####3æà#####<#####>#"###@#####B#####H#H#####L##ÿôÿô#X#

#E#(#ü#####H#H#####0#(#####d#####'#####h#####
#####X#÷ôÄ#l#<ôÀ÷#@#p#####'#####
#####ô#ð0###9###B# #g## ####,###1###8###3###:###9###C#####à#0#x#####Dÿÿÿÿ##' #
###>ÿp###p#2#####Pí*#### (### + -⁰Ä^a«μ²¿»»³/₄¹/₂»¹/₄ÄÄμ-
ÄÁ§ŋÄ°°¹ŋ»⁰ - ° - i π Ä | e####%-BR0Ugh²μ lz - Ë Ì Ä Ë Ë »¹/₄Æ»¿uqN%###0 Ê×¹/₄¹/₂ÇÈ¿Á««Ç
İÑ¬^Gvç25Gg\T#*Bh²Äàÿ#####àò0h#«##+ ' ³Ü####à
ò0h#«##+ ' ³Ü0###Ä#####x#####
'#####³/₄### ###Î#####Ü###

###a#####ò#####p#####(#####

###Mabry
Tyson#####Barbera#####2###@###ê#jB°½#@###
#####@###q£mB°½#####Microsoft PowerPoint
4.0##G#####pyÿÿPICT##I###ÿ

#ÿp###@###@##÷□ôÄ#ł#<##### #□#####
÷□ôÄ#ł#<#2÷□ôÄ#ł#<# #□#,#

Helvetica#####À#.#####@#@#@#####(ø³öß/Explaining & Recovering
from Computer Break-ins# #[]# #[]##### ù#ÿ<#-ÿ<# #[]# #[]##### ÿøôÅÿø
Ô# #[]# #[]#####==èè## #####(#¾ø\#Impact## #[]# #[]##üü##(#####
#[]#####(#Æôì#¥#####)Ø!DoD Information Security improved#####
#ĐŏĂ#Đp/#####ð##(#Æp.# by #####(#IŏĂ\$DERBI providing expertise to widely
#####*&distributed, minimally trained System #####*[]#Administrators
###üü##(#####(##ôì#¥#####)Ø#Crisis response improved#
##ŏĂ##ûè##### ##(##ûè

by current #####(#ö\$information distributed via
database###üü##(#####(#Tôì#¥#####)Ø#Downtime and exposure minimized##
#^öÄ#^p!#####D##(#Tp # by #####(#xöÄ#nullifying current
attacks###üü##(#####(#ôì#¥#####)Ø#Situation awareness raised# #çöÄ#
çü6#####p##(#ü6# by reporting #####(#öÄ#coverage and accuracy# # #
######(#Ê#a# #####==èè## #####)(#Schedule# # ######0# #,#
`# # # #0# #,#è
`# # # #yyyy# #%#À|#À# # # #%#D#|#D# # # #####(
ç#ü#FY00## # # #####(#ç###FY99## # # #####(#ç#

#FY98## # # # % # ° # | # ° # # # # # ==èè## #####(ùp# New Ideas##üü##(#####
######(ú:ÿü#¥#####)Ø#Forensic analysis## úD#ÔúD#####P##(ú:### of
intrusions uses #####(ú¾#Ô(database of current vulnerabilities and
#####*#exploits#####(ü#ÿü#¥#####)Ø#Analysis drives ##À##(ü##
ç#explanation-based# ü##fü# ###(ü# ## #####(ü#Ô#recommendation of steps
for ###üü##(##`##(ü#Ô#recovery## ü#Ôü ñ##### ##(ü ñ# #####(ý

#0#and ###üü##((## ##(ý

prevention## ý##Ûý##i#####(ýÏÿü#¥#####)Ø#Automated reporting##
ýØ#ÛýØ#£#####À##(ýÏ#Å

from sites #####(pR#0#updates database used in analyzing #####*#subsequent
attacks# # # # #==èè# #p#µ#p
#à#u#à
#À# #À
#\#####`#####(# # # # #Exploit database## # # # # # # # # #==èè# # # # #µ#
#\#####`#####(Î# # # # #Explanation and#####*b#
reporting# # # # #\#####(®# # # # #Evidential correlations#####*b# among
indicators## # # # #\#####(h# # # # #Intrusion indicators #####*p# knowledge
base## # # # # #==èè# #D# #D
#\#####`#####Times#####\#####(##øÇ?Artificial Intelligence Center,
SRI International: Mabry Tyson# # # # #\#####`#####(x# # # # #Recovery and
repair# # # # # #==èè##### #l#µ#l### # # # # #µ# #0# # # # #
#Û#u#Û#0# # # # # #Î#U#Î

#0### #\#µ#\#Ä# # # # #|#µ#|#ä# # # # # #Î# #Î#ä# # # # # # # # # #
d# # # # # #~#u#~ Ä# # # # #\#####"#l#u/## # # # # "#l/#/## # # # # "#l
 /## # # # # "#l
%/## # # # # "# #¥/## # # # # "# 5/## # # # # "# Å/## # # # # "#
U/## # # # # #i#d#

[illegible]

#####!##x#!ü`úà###h###i###0##0###è#####ÝÝ###
ùDöôÿ´p##□#
ùTùçùTùç# #£# #¾#q#□û. ú□ýáúðýáú,ýáú`ýáú□ýYú□ýIú□ý#ú□üÉú□ü,ú□ü□ú□ü#ú□û□ú□ú_ú□û0ú□
úFú□ú6ú□ú.ú□ú.ú.ú.úðú6úàúFúàú0úàú_úàú□úàú#úàú□úàú_úàúÉúàý!
úéý9úðýIúðýáúðýáúÁýáú_#"ùTùç### #¿# #i#####i#¶#####@# # #i#÷#####
#####"ýáú°#####è###à#####0###□###□#!ùÍú□###□###ß###ø#####
#####!##x#!ü`úà###h###i###0##0###è##### #£# #¾###
ùDöôÿ
´p#####i#¶#####@#"ýáú_###i#¶#####@#####p#□û. ú□ýáúðýáú,ýáú`ýáú□ýYú□ýIú□ý
#ú□üÉú□ü,ú□ü□ú□ü#ú□û□ú□ú_ú□û0ú□úFú□ú6ú□ú.ú□ú.ú.ú.úðú6úàúFúàú0úàú_úàú□úàú#úàú□úàú
úàúÉúàý!úéý9úðýIúðýáúðýáúÁýáú# #¿# #i#####i#¶#####@# # #i#÷#####
#####"ù6ú`#### ######!##x#!ùhú0###h###i##### #£# #¾###
ùDöôÿ
´p#####i#¶#####@#"ýQúè###i#¶#####@#####p#>ù6ú°ýQúèù6ú°ù6úÉù>ùðù0ùðùWùðù
gùðù□ùðù#ùðù□ùðùÁùðùðùðý!úàýQúè# #¿# #i# #□# #□#####ù\øN###"□
S□□øø##"ù¾÷¥###i#0####@##i#0####@## #x#####ùPøÎ###i#Ê#####i#Ê#####`#`r-
##>>>>>>>###0#0#Aù¾÷¥úíùç#####i#¶#####@#####H# #Ê#i#0####@## #x# #ù####
#"□S□□øø#i#0####@##i#0####@## #¾# #ù#####i#¶#####@##>>>>>>>#q#¶ùμ□ùíøöù×ø¶
ùßø¶ùßø¶ùçø¶ùçø¶ùçøøùíøøùíø!ùíø!ùíø□ùíø□ùíø□ùíø□ùíø□ùçø□ùçø□ùçø□ùßø□ùßø□ù×ø□ù×ø□
ùÍøÆùÍøÆùÁøÆùÁøÆù½øÆù½øÎù½øÎùμøÎùμø0ùμø0ùμøPùμøPù½øæù½øæù½øíù½øíùÁøíùÁøíùÍøöùÍøö
ù0øöù×ø¶#"ù×ø¶###i#¶#####@#####p#¶ùμ□ùíøöù×ø¶ùßø¶ùßø¶ùçø¶ùçø¶ùçøøùíøø
ùíø!ùíø!ùíø□ùíø□ùíø□ùíø□ùíø□ùíø□ùçø□ùçø□ùçø□ùßø□ùßø□ù×ø□ù×ø□ùÍøÆùÍøÆùÁøÆùÁøÆù½øÆù½øÎ
ù½øÎùμøÎùμø0ùμø0ùμøPùμøPù½øæù½øæù½øíù½øíùÁøíùÁøíùÍøöùÍøöù0øöù×ø¶#i#0####@## #¿#
#ù# #x# # #i#÷#####
üXùWù□ùø#!ú□ù□#!ùÍù□###x###à0##Àø##·ø##ø#####
#####Y###(###1#!ú□ùg#!ù□ù0#!ùPù7#####>>>>>>>###
ùDöôÿ´p##□#
ù\øNù\øN# #£# #¾#q#□ùløöüXù□üXùWùPùWù8ùWùíù_ù□ùgù#ùwù□ù□ù-ù□ùYù□ùÀù□ù½ù□ù□ù□ù|
ù□ùtùgùlù#ùlù#ùlùßù□ùøù□ù#ù□ù'ù□ù0ù□ùgù□ù□ù½ù□ùÀù□ùåù□ù5ùwù□ùgù#ùWù□ùGùíù?
ù8ù7ùPù7ùXù7ùXùW#"ù\øN### #¿# #i#####i#¶#####@# # #i#÷#####
üXùWù□ùø#!ú□ù□#!ùÍù□###x###à0##Àø##·ø##ø#####
#####Y###(###1#!ú□ùg#!ù□ù0#!ùPù7##### #£# #¾###
ùDöôÿ
´p#####i#¶#####@#####i#¶#####@#####p#□ùløöüXù□üXùWùPùWù8ùWùíù_ù□ùgù#ùwù
□ù□ù-ù□ùYù□ùÀù□ù½ù□ù□ù□ù|
ù□ùtùgùlù#ùlù#ùlùßù□ùøù□ù#ù□ù'ù□ù0ù□ùgù□ù□ù½ù□ùÀù□ùåù□ù5ùwù□ùgù#ùWù□ùGùíù?
ù8ù7ùPù7ùXù7ùXùW# #¿# #i#####i#¶#####@# # #i#÷#####
#####"ùÿù ###!ùÀù□#####è##àx###è#####ð##### #£# #¾###
ùDöôÿ´p#####i#¶#####@#####i#¶#####@#####p#"ùtøpù÷ù□ù÷ù_ùÀù□ù□ù□ù□ùwù|
ù_ùtøp# #¿# #i# # #i#÷#####
#####"ù`ù_####øX#####ð###è###□9##`ø##è##øß###ð#####0à##
###0ð###Ê#####Q#####ÝÝ###
ùDöôÿ´p##□#
ù\øNù\øN# #£# #¾#q#^üPøVý ù_üXù_ü_ùWùÀù/ùðù'üéøpý#øÎý
ø□ùùøvüñøfùàøVüðøVüÀøVü_ø^ü_øvü ø|ü□øÆü□øæùpù#ùXù#ùPù#ùXù_"ù\øN### #¿# #i#
#####i#¶#####@# # #i#÷#####
#####"ù`ù_####øX#####ð###è###□9##`ø##è##øß###ð#####0à##
###0ð###Ê#####Q##### #£# #¾###
ùDöôÿ´p#####i#¶#####@#"ùXù_###i#¶#####@#####p#^üPøVý
ù_üXù_ü_ùWùÀù/ùðù'üéøpý#øÎý_ø□ùùøvüñøfùàøVüðøVüÀøVü_ø^ü_øvü ø|ü□øÆü□øæùp
ù#ùXù#ùPù#ùXù_# #¿# #i# # #i#÷#####
#####"ùðù#À)##_ð##èß##8###`ð###ð#####) #####LÍLðÿÿ###
ùDöôÿ´p##□#
ù\øNù\øN# #£# #¾#q#6ù□øfùñù7ü°ù7üéøæùñøÆùñø□üðøñüÈøfùÈø~üÀø□ü°øÎù□ù#ù°ù7#"ù\øN##
#¿# #i#####i#¶##### # #i#÷#####
#####"ùðù#À)##_ð##èß##8###`ð###ð#####) ##### #£# #¾###
ùDöôÿ
´p#####i#¶#####i#¶#####p#6ù□øfùñù7ü°ù7üéøæùñøÆùñø□üðøñüÈøfù
Èø~üÀø□ü°øÎù□ù#ù°ù7# #¿# #i#####i#¶#####@# # #i#÷#####
#####"ù øÎ####ð###à###è###è##### #£# #¾###
ùDöôÿ´p#####i#¶#####@#####i#¶#####@#####p##ü øñüÀøÎü øÎü`ø|ü_ø□üÀøñ# #¿
#i#"□S□□øø#####"ù÷øÎ###i#0####@##i#0####@## #x#####ùøæ###i#Ê#####i#Ê

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```

[]#wwwwwww#AújùúüüR####i#l#####@#####H#É#i#0####@## #x# #ù#
###"□C°øø#i#0####@##i#0####@## #3# #ù#####i#l#####@##wwwwww#wq##u5úúú|ü*ú5
ü"ú|ü*ú|ü#ú5úúú5ü#"ú5ü"###i#l#####@#####p##u5úúú|ü*ú5ü"ú|ü*ú|ü#ú5úúú5
ü"#i#0####@## #¿# #ù# #x#####i#l#####@#####"ú=úú#i# #[]# #[]#[]äy[]y#####
#####H###H#####3-
T#####[]#y##yyyyyy##yyýýlì##yyýý[]#yyýýff##yyýý33##yyýý####yyìyy##yyìììì##
yyì[]#yyìff##yyì33##yyìl####yy[]yy##yy[]lì##yy[]ff##yy[]33##yy[]####yy
yffyy##yyfflì##yyff[]#yyffff##yyff33##yyff####yy33yy##yy33lì##yy33[]#yy33ff##yy
y3333##yy33####yy##yy##yy##lì##yy##[]#yy##ff##yy##33##yy#####lìyyýý##lìyyýlì##lì
lìyy[]#lìyyff##lìyy33##lìyy####lìlìyy##lìlìlì##lìlì[]#lìlìff##lìlì33##lìlì####lì
lì[]yy##lì[]lì##lì[]ff##lì[]33##lì[]####lìffyy##lìfflì##lìff[]#lìffff##lì
lìff33##lìff####lì33yy##lì33lì##lì33[]#lì33ff##lì3333##lì33####lì##yy##lì##lì##lì
lì##[]#lì##ff##lì##33##lì#####[]yyýý##[]yylì##[]yy[]#[]yyff##[]yy33##[]yy####
[]lìyy##[]lììì##[]lì[]#[]lìff##[]lì33##[]lì####[]yy##[][]lì##[]ff##[]
[]33##[]ffyy##[]fflì##[]ff[]#[]ffff##[]ff33##[]ff####[]33yy##[]33lì##
[]33[]#[]33ff##[]3333##[]33####[]#yy##[]#lì##[]#[]#[]#ff##[]#33##[]#####f
fyyýý##ffyylì##ffyy[]#ffyyff##ffyy33##ffyy####fflìyy##fflìlì##fflì[]#fflìff##f
flì33##fflì####ff[]yy##ff[]lì##ff[]ff##ff[]33##ff[]####ffffyy##ffflì##ff
fff[]#ffflìff##ffflì33##ffflì####ff33yy##ff33lì##ff33[]#ff33ff##ff3333##ff33####f
f##yy##ff##lì##ff##[]#ff##ff##ff##33##ff#####33yyýý##33yylì##33yy[]#33yyff##3
3yy33##33yy####33lìyy##33lìlì##33lì[]#33lìff##33lì33##33lì####33[]yy##33[]lì##3
3[]ff##33[]33##33[]####33ffyy##33fflì##33ff[]#33ffff##33ff33##33ff####3
333yy##333lì##3333[]#3333ff##333333##3333####33##yy##33##lì##33##[]#33##ff##3
3##33##33#####yyýý####yylì####yy[]####yyff####yy33####yy#####lìyy####lìlì##
#lì[]####lìff####lì33####lì#####[]yy####[]lì####[]ff####[]33####[]####
#ffyy####fflì####ff[]####ffff####ff33####ff#####33yy####33lì####33[]####33ff##
#3333####33#####yy####lì#####ff#####33##î#####Yÿ#####»»#####a
a#####[]#####w#####U#####D##### "#####î#####Yÿ#####»»#####
#a#####[]#####w#####U#####D##### "#####î#####Yÿ#####»»###
###a#####[]#####w#####U#####D##### "#####îîîîî##YÿYÿYÿ##»»»»»»##a
aaaaa##[]#####w#####U#####D##### "#####yÿy####ûßöÛÿ»b##$#
,ûßöÛÿ»b#ûßúxp#ÿÿûcöûúx#ÿÿûxp#ÿÿ»öûúx#ÿÿÿ#[]#[]#[]#

```

ô#âÿ[]#ô#üÿú#
ø#Éÿ[]#Þÿü#
û#¼ÿ¥#Çÿþ##ý#°ÿÄ#
´ÿ#####¥ÿí#[]ÿ#####[]ÿ[]ÿ####[]ÿ[]ÿ#####[]ÿ[]ÿ#####[]ÿ[]ÿ#####[]ÿ[]ÿ#þ#[]ÿ ÿ#ý#[]ÿ
çÿ###ü#[]ÿ£ÿ###ú#[]ÿ«ÿú##ö#[]ÿµÿô##ó#[]ÿÂÿê##î#[]ÿÏÿå##é#[]ÿÔÿâ##å#[]ÿÛÿà##ã#[]ÿßÿÿ##á#[]
ÿãÿÛ##à#[]ÿåÿÛ##ß#[]ÿçÿÛ##Þ#[]ÿéÿø##Þ#[]ÿéÿø##Þ#[]ÿêÿ×##Þ#[]ÿêÿ×##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#
[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#[]ÿìÿô##Ý#
#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##
Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##
#Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##Ü#[]ÿìÿô##
##Ü#[]ÿðÿô##Ü#[]ÿðÿô##Ü#[]ÿðÿô##Ü#[]ÿñÿô##Ü#[]ÿñÿô##Ü#[]ÿñÿô##Ü#[]ÿñÿô##Ü#[]ÿðÿô##Ü#[]ÿóÿ
ô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿô##Ü#[]ÿóÿ
ÿÑ##ô#[]ÿ÷ÿð##ô#[]ÿøÿÏ##ô#[]ÿøÿÏ##×#[]ÿúÿÏ##ô#[]ÿüÿÏ##ô#[]ÿýÿÏ##ô#[]ÿþÿÏ##ô#[]ÿ#ÿË##ô#[]ÿ
Ë##ô#[]ÿË##Ñ#[]ÿË##Ð#[]ÿÇ##Ï#[]ÿÆ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#[]ÿÅ##Ï#
Å#[]ÿ>##Å#[]ÿ°##Å#[]ÿ¹##Å#[]ÿ¨ÿ·##¼#[]ÿµ##¼#[]ÿ³##¹#[]ÿ°##·#>ÿ##
´#Åÿª##±#Çÿ§##¬#Îÿ¥##§#Ûÿ[]##î#éÿ[]##[]#úÿ[]##î#[]#

ÜPùGÿKù#####"ÜPùG### #[]#i#[]##ÿi[]ÿÿR###ÿÿ#####,# #÷#Impact####÷#####Ráj#
02##°»#(üÔùR#D## #[]# #[]##Ä[]#+[]#E## #[]# #[]##°»#(pùR#R## #[]# #[]##°»#*[]B# #[]# #[]
##°»#*[]# ###c[])##I## #[]# #[]#####i#[]#

ü h ù ü ñ û y # " ü h ù ##### # i # # # y ó k # # u # # # y ÿ # # # # , # # * Ý # Arial Black # # * Ý # #

Õ#(üôù iagnosis,# # # #####i#

#####

ý#`ùýûâ#"ý#`ù### #i#öó###{###ÿÿ####(ýmù#xplanation,# # ######
#####i#

#####

ýùp"ûA#"ýù### #i###ÿò##q##ÿÿ####
##i##

Õ#+##ecover# ##

#####

p*ùp»ú°#"p*ù### #i#i#yò¼###i###yÿ#####+#reak-# # ######i#
#

#####

pĚùŸSú##"pĚù### #i###ÿò·##_##ÿŸ###
i##

Õ#(ÿ7ù#ns## # ######

#####

ý©ûap#ü"#"ý©ûa### #[]#i#[]##ÿõ[]#ÿÿ[]###ÿÿ[] [] [] ## ##pİ#(ýýûd#from## #[]# #[]#####

#[]#i#d#

PPNT##### #[]# #[]#ÿw₂####

```
#####bpyybyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
#####BarberaUI0x+eöðç00äëóíóíPá0éíññç+ëxãçUA
Ð00YáääääU0N0äëëU00íöð####öüÿ+úpüðöþðöÿyüöëöüÿÿüðçÍ0äëñóUÿUU0ÐNÜ0U0Í0ÏYáäé×Ä¿
E0ääUáUÉÍIUëëá0ÄÊÊÎÑÉ0UÎÎBêPN0äççáUæðëäëç0UíëäëYÉ0ÍYUUÍÄÄÍäU#####
```

#!* /<@FK0pQ#RNN#4##p#□#####
##

```
# #0,(76%# 2±°0ăăăăăöëÜlîññîëlîiîi16ôôðîðîñëÜSăăYăYôîĀĀĀ,|¥ i®ºº¿-
©|'²º.°µ¶-ꝑ©¶ĴĀĀĀĴ²²¹»ĀĒ½¶¥³$¥-µ'²□□©,ĀĒĒĒĒ»Ā¹®□«®»-¹«□$'¹Ē□$□i□□□□|¥
£□□□□□□□-¶³µ¼ĀŌĐ½µ¹·¶
'':|□□□□□□□|¬²¥$²½Ā·ĀĒµ±|µ¼·»¹ĈĒ¶¼ĀĒĀ³ĀĪŌŌUŪŌŌŌŌNŪŪàĐĈÇĀĒĒĪ±²µ°µ³®·ĀĒ¼+¾ĀĀ¹¿»»□
·µµ£³-|²Ī¹'¿,□□□¶Ē³ĀŌŌUŪŌĪĀĒĒŌŪŪPèàèİC#u#r#r#e#n#t#
#I#D#####y#####
#####S#u#m#m#a#r#y#I#n#f#o#r#m#a#t#i#o#n#####
#####(###y#####p#####
#####y#####
ÿ#####
#####y#####
#####
```